

W 2182EM

JP2003337749**Patent number:** JP2003337749**Publication date:** 2003-11-28**Inventor:****Applicant:****Classification:**

- International: G06F1/00; G06F12/14; G06K19/073; G09C1/00;
G06F1/00; G06F12/14; G06K19/073; G09C1/00; (IPC1-
7): G06F12/14; G06F1/00; G06K19/073; G09C1/00

- european:

Application number: JP20030067248 20030312**Priority number(s):** JP20030067248 20030312; JP20020068097 20020313

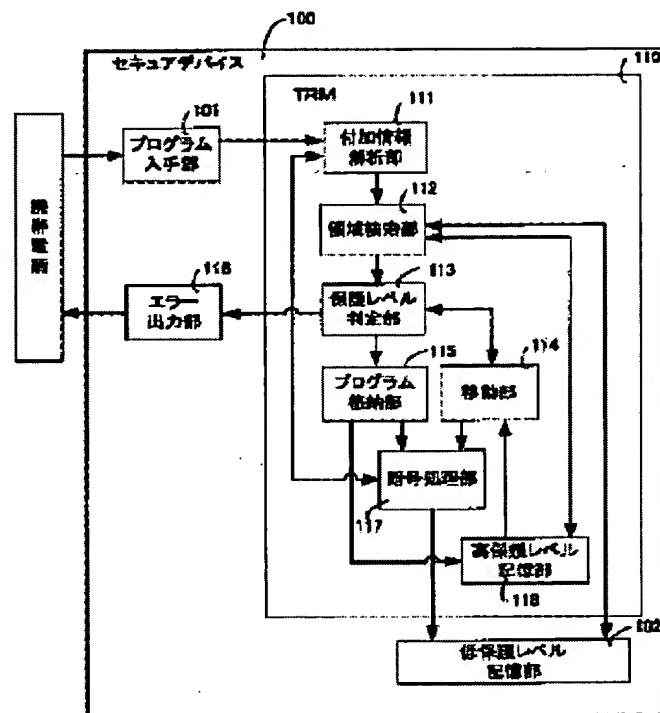
Report a data error here

Abstract of JP2003337749

PROBLEM TO BE SOLVED: To provide a secure device capable of downloading a program above a capacity of a storage area mounted inside a TRM while securing safety necessary for a manager of each program.

SOLUTION: This secure device 100 storing the program for making it available for use is provided with a low protection level storage part 102, a high protection level storage part 118, a program acquisition part 101 acquiring a program including additional information for specifying a storage destination, an additional information analysis part 111 storing a program matching the additional information in a storage part specified by the acquired additional information, an area retrieval part 112, a protection level determination part 113, and a program storage part 115.

COPYRIGHT: (C)2004,JPO



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-337749

(P2003-337749A)

(43) 公開日 平成15年11月28日 (2003. 11. 28)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 K 5 B 0 1 7
			3 1 0 H 5 B 0 3 5
1/00		G 0 9 C 1/00	6 6 0 D 5 B 0 7 6
G 0 6 K 19/073		G 0 6 K 19/00	P 5 J 1 0 4
G 0 9 C 1/00	6 6 0	G 0 6 F 9/06	6 6 0 F
審査請求 未請求 請求項の数25 O L (全 17 頁)			

(21) 出願番号 特願2003-67248 (P2003-67248)

(22) 出願日 平成15年3月12日 (2003. 3. 12)

(31) 優先権主張番号 特願2002-68097 (P2002-68097)

(32) 優先日 平成14年3月13日 (2002. 3. 13)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 松崎 なつめ

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 佐久嶋 和生

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100090446

弁理士 中島 司朗

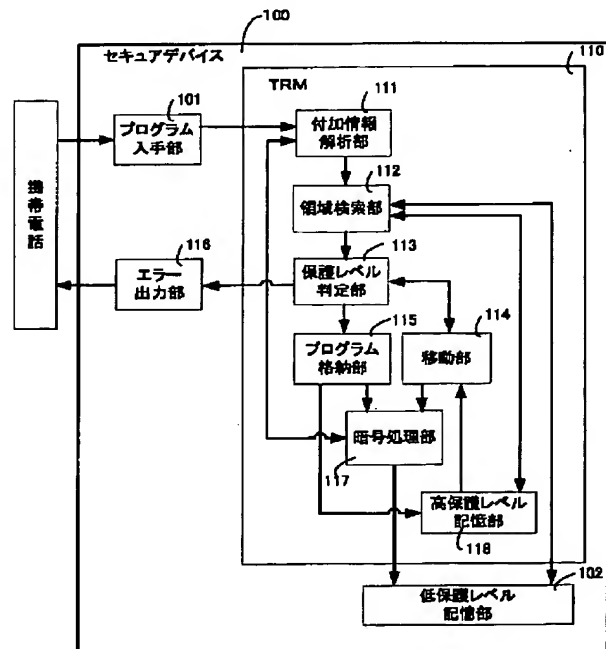
最終頁に続く

(54) 【発明の名称】 セキュアデバイス

(57) 【要約】

【課題】 TRM内に実装する記憶領域の容量を越えるプログラムを、各プログラムの管理者が必要とする安全性を確保しつつ、ダウンロードすることができるセキュアデバイスを提供する。

【解決手段】 プログラムを格納して利用に供するセキュアデバイス100であって、低保護レベル記憶部102と、高保護レベル記憶部118と、格納先を特定するための付加情報を含むプログラムを入手するプログラム入手部101と、入手された付加情報により特定される記憶部に当該付加情報に対応するプログラムを格納する付加情報解析部111、領域検索部112、保護レベル判定部113、及びプログラム格納部115とを備える。



【特許請求の範囲】

【請求項1】 デジタルデータを格納して利用に供するセキュアデバイスであって、それぞれが記憶領域を備える複数の記憶手段と、格納先となる記憶手段を特定するための格納先情報が付加されたデジタルデータを入手する入手手段と、前記格納先情報により特定される記憶手段に、前記デジタルデータを格納する処理手段とを備えることを特徴とするセキュアデバイス。

【請求項2】 前記複数の記憶手段には、それぞれ保護レベルが設定されており、前記格納先情報は、保護レベルを示し、前記処理手段は、前記格納先情報が示す保護レベルと同じ保護レベルが設定されている記憶手段を、前記デジタルデータの格納先として特定することを特徴とする請求項1に記載のセキュアデバイス。

【請求項3】 前記複数の記憶手段には、それぞれ保護レベルが設定されており、前記格納先情報は、保護レベルを示し、前記処理手段は、前記格納先情報が示す保護レベル以上の保護レベルが設定されている記憶手段のうちの1つを、前記デジタルデータの格納先として特定することを特徴とする請求項1に記載のセキュアデバイス。

【請求項4】 前記処理手段は、前記入手手段により入手された格納先情報が示す保護レベル以上の保護レベルが設定された記憶手段のうち、前記デジタルデータを格納するための空いている記憶領域を確保できる記憶手段を全て検索する検索手段と、検索手段により検索された記憶手段のうち、一番高い保護レベルが設定されている記憶手段を前記デジタルデータの格納場所として決定する決定手段と、前記デジタルデータを、決定手段により決定された記憶手段に格納する格納手段とを含むことを特徴とする請求項3に記載のセキュアデバイス。

【請求項5】 前記処理手段は、さらに、前記検索手段により何れの記憶手段も検索されなかった場合に、利用者にデジタルデータを格納できない旨を提示するためのエラー情報を出力する出力手段を含むことを特徴とする請求項4に記載のセキュアデバイス。

【請求項6】 前記処理手段は、さらに、前記検索手段により何れの記憶手段も検索されなかった場合に、(1)前記入手手段により入手された格納先情報が示す第1保護レベル以上の保護レベルが設定されている記憶手段に格納されているデジタルデータのそれぞれに付加された格納先情報を読み出し、(2)読み出した格納先情報のうち、それぞれの格納先情報が示す保護レベルが、当該第1保護レベルよりも低い格納先情報を抽出し、(3)抽出した格納先情報に対応するデジタル

データを、当該第1保護レベルよりも低く、且つ、それぞれの格納先情報が示す保護レベル以上の保護レベルが設定されている記憶手段に移動することにより、前記入手手段により入手されたデジタルデータを格納するための記憶領域を確保する移動手段を含み、

前記格納手段は、移動手段により確保された記憶領域に、前記入手手段により入手されたデジタルデータを格納することを特徴とする請求項4に記載のセキュアデバイス。

【請求項7】 前記移動手段により読み出された格納先情報は、デジタルデータを移動する場合に暗号化するか否かを指定し、前記移動手段は、移動すべきデジタルデータに付加された格納先情報に従い、当該デジタルデータを暗号化して移動するか、又は、そのまま移動することを特徴とする請求項6に記載のセキュアデバイス。

【請求項8】 前記移動手段により読み出された格納先情報は、デジタルデータを移動する場合にデジタルデータに改竄検出用の情報を付加するか否かを指定し、前記移動手段は、移動すべきデジタルデータに付加された格納先情報に従い、当該デジタルデータに改竄検出用の情報を付加して移動するか、又は、そのまま移動することを特徴とする請求項6に記載のセキュアデバイス。

【請求項9】 前記移動手段により読み出された格納先情報は、デジタルデータを移動する際にデジタルデータにデジタル署名を埋め込むか否かを指定し、前記移動手段は、移動すべきデジタルデータに付加された格納先情報に従い、当該デジタルデータにデジタル署名を埋め込んで移動するか、又は、そのまま移動することを特徴とする請求項6に記載のセキュアデバイス。

【請求項10】 記処理手段は、さらに、前記移動手段により記憶領域を確保できない場合に、利用者にデジタルデータを格納できない旨を提示するためのエラー情報を出力する出力手段を含むことを特徴とする請求項6に記載のセキュアデバイス。

【請求項11】 前記複数の記憶手段には、それぞれ保護レベルが設定されており、前記格納先情報は、保護レベルを示し、さらに、前記対応するデジタルデータの格納先として、当該保護レベルが設定されている記憶手段のみを格納先として特定するか、及び、当該保護レベルが設定されている記憶手段以上の保護レベルが設定された記憶手段を格納先として特定するかのどちらかを指定し、

前記処理手段は、前記格納先情報に従い、前記格納先情報が示す保護レベルが設定されている記憶手段を、又は、前記格納先情報が示す保護レベル以上の保護レベルが設定されている記

憶手段のうちの1つを、前記デジタルデータの格納先として特定することを特徴とする請求項1に記載のセキュアデバイス。

【請求項12】 前記格納先情報は、前記対応するデジタルデータの格納先を、当該セキュアデバイスにおいて格納する際に任意に決定してもよいかを指定し、前記処理手段は、前記格納先情報に従い、任意に決定する記憶手段に、又は、前記格納先情報により特定される記憶手段に、前記デジタルデータを格納することを特徴とする請求項1に記載のセキュアデバイス。

【請求項13】 前記複数の記憶手段には、それぞれ保護レベルが設定されており、前記格納先情報は、デジタルデータを所定の保護レベル以下の記憶手段に格納する際に暗号化するか否かを指定し、

前記処理手段は、デジタルデータを前記所定の保護レベル以下の記憶手段に格納する際に、前記格納先情報に従い、当該デジタルデータを暗号化して格納するか、又は、そのまま格納することを特徴とする請求項1に記載のセキュアデバイス。

【請求項14】 前記複数の記憶手段には、それぞれ保護レベルが設定されており、前記格納先情報は、デジタルデータを所定の保護レベル以下の記憶手段に格納する際にデジタルデータに改竄検出用の情報を付加するか否かを指定し、

前記処理手段は、デジタルデータを前記所定の保護レベル以下の記憶手段に格納する際に、前記格納先情報に従い、当該デジタルデータに改竄検出用の情報を付加して格納するか、又は、そのまま格納することを特徴とする請求項1に記載のセキュアデバイス。

【請求項15】 前記複数の記憶手段には、それぞれ保護レベルが設定されており、前記格納先情報は、デジタルデータを所定の保護レベル以下の記憶手段に格納する際にデジタルデータにデジタル署名を埋め込むかを指定し、

前記処理手段は、デジタルデータを前記所定の保護レベル以下の記憶手段に格納する際に、前記格納先情報に従い、当該デジタルデータにデジタル署名を埋め込んで格納するか、又は、そのまま格納することを特徴とする請求項1に記載のセキュアデバイス。

【請求項16】 前記複数の記憶手段には、それぞれ保護レベルが設定されており、前記格納先情報は、前記デジタルデータの優先度を示し、少なくとも1つの記憶手段には、デジタルデータが格納され、

記憶手段に格納されているデジタルデータには、デジタルデータの優先度が設定され、

記憶手段には、より優先度が高いデジタルデータがより保護レベルが高い記憶手段に格納されている状態で、デジタルデータが格納されており、

前記処理手段は、前記格納先情報により示される優先度に基づいて、前記状態を維持したまま、前記入手手段により入手されたデジタルデータを格納することを特徴とする請求項1に記載のセキュアデバイス。

【請求項17】 記憶手段に格納されているデジタルデータには、デジタルデータの優先度を示す格納先情報が付加されており、

前記処理手段は、一番高い保護レベルが設定されている記憶手段から順に、(1)前記入手手段により入手されたデジタルデータを格納するための空いている記憶領域を確保できるかを判定し、(2)判定が否定的な場合に、判定対象の記憶手段に格納されているデジタルデータのそれぞれに付加された格納先情報を読み出し、(3)読み出した格納先情報のうち、それぞれの格納先情報が示す優先度が、前記入手手段により入手された格納先情報が示す優先度よりも低い格納先情報を抽出し、(4)抽出した格納先情報を含むデジタルデータを、移動するデジタルデータ対応する保護レベルより低い保護レベルが設定されている記憶手段に移動し、(5)前記判定が肯定的となるまで(1)～(4)の処理を繰り返すことにより、前記入手手段により入手されたデジタルデータを格納するための記憶領域を確保する移動手段と、

移動手段により確保された記憶領域に、前記入手手段により入手されたデジタルデータを格納する格納手段とを含むことを特徴とする請求項16に記載のセキュアデバイス。

【請求項18】 前記移動手段により読み出された格納先情報は、デジタルデータを移動する場合に暗号化するか否かを指定し、

前記移動手段は、移動すべきデジタルデータに付加された格納先情報に従い、当該デジタルデータを暗号化して移動するか、又は、そのまま移動することを特徴とする請求項17に記載のセキュアデバイス。

【請求項19】 前記移動手段により読み出された格納先情報は、デジタルデータを移動する場合にデジタルデータに改竄検出用の情報を付加するか否かを指定し、前記移動手段は、

移動すべきデジタルデータに付加された格納先情報に従い、当該デジタルデータに改竄検出用の情報を付加して移動するか、又は、そのまま移動することを特徴とする請求項17に記載のセキュアデバイス。

【請求項20】 前記移動手段により読み出された格納

先情報は、デジタルデータを移動する際にデジタルデータにデジタル署名を埋め込むか否かを指定し、前記移動手段は、

移動すべきデジタルデータに付加された格納先情報に従い、当該デジタルデータにデジタル署名を埋め込んで移動するか、又は、そのまま移動することを特徴とする請求項17に記載のセキュアデバイス。

【請求項21】 前記格納先情報は、さらに、保護レベルを示し、

前記移動手段は、

前記入手手段により入手された格納先情報が示す保護レベルより低い保護レベルが設定されている記憶手段においては、前記処理を行わず、

前記処理手段は、さらに、

移動手段により記憶領域を確保できない場合に、利用者にデジタルデータを格納できない旨を提示するためのエラー情報を出力する出力手段を含むことを特徴とする請求項17に記載のセキュアデバイス。

【請求項22】 前記入手手段により入手されるデジタルデータはコンピュータプログラムであり、複数のサブプログラムを含み、サブプログラム毎に格納先情報が付加されており、

前記処理手段は、

サブプログラム毎に、それぞれに付加された格納先情報により特定される記憶手段に、対応するサブプログラムを格納することを特徴とする請求項1に記載のセキュアデバイス。

【請求項23】 前記複数の記憶手段には、それぞれ保護レベルが設定されており、

前記入手手段により入手されるデジタルデータはコンピュータプログラムであり、1つのメインルーチンと複数のサブルーチンを含み、各ルーチン毎に格納先情報が付加され、特にメインルーチンに付加された格納先情報は保護レベルが高い記憶手段に格納すべき事を示し、

前記処理手段は、

ルーチン毎に、それぞれに付加された格納先情報により特定される記憶手段に、対応するルーチンを格納することを特徴とする請求項1に記載のセキュアデバイス。

【請求項24】 前記入手手段により入手されるデジタルデータには、

当該デジタルデータに付加された格納先情報の正当性を示し、又は、当該デジタルデータと格納先情報の対応が正しいことを示すデジタル署名が埋め込まれているか、又は、認証子が付加されており、

前記処理手段は、

前記デジタル署名、又は、認証子に応じた認証を実施し、当該認証が成功した場合に限り、前記デジタルデータを格納することを特徴とする請求項1に記載のセキュアデバイス。

【請求項25】 デジタルデータを格納して利用に供す

るセキュアデバイスにおける格納方法であって、

前記セキュアデバイスは、それぞれが記憶領域を備え、当該格納方法は、

格納先となる記憶手段を特定するための格納先情報が付加されたデジタルデータを入手する入手ステップと、前記格納先情報により特定される記憶手段に、前記デジタルデータを格納する処理ステップとを含むことを特徴とする格納方法。

【発明の詳細な説明】

10 【0001】

【発明の属する技術分野】本発明は、コンテンツの不正な使用を防止するための技術、及び、電子商取引（モバイルEC）における不正を防止する技術を備えるセキュアデバイスに関する。

【0002】

【従来の技術】近年、インターネット等のネットワークを介して、音楽コンテンツや動画コンテンツの配信を受けるコンテンツ配信サービス、及び、モバイルECサービス等の様々な電子情報サービスが普及している。これらの電子情報サービスにおいては、コンテンツの不正な使用を防止するコンテンツ保護技術、及び、モバイルECにおける認証技術や課金技術等のEC保護技術が不可欠であり、これら技術を備えるセキュアデバイスが開発され利用されている。

20 【0003】例えば、利用者はこのようなセキュアデバイスを自分の携帯電話に装着して、外出先からコンテンツ配信サービスやモバイルECサービス等を安全に行うことができる。セキュアデバイスについては、「コンテンツ配信・モバイルコマース用のセキュアマルチメディアカード」日立評論2001年10月号、三宅順、石原晴次、常広隆司に、コンテンツ保護技術とEC保護技術とを備えるセキュアマルチメディアカード（以下「SM-MC」）が記載されている。

【0004】SMMCには、J A V A（登録商標）C a r dのようにプログラムのダウンロード機能を備えるタイプがある。ここでダウンロードされるプログラムは、新規アプリケーションプログラムや、カード内に記録されているプログラムのバージョンアップ版等である。プログラムのダウンロード機能を備えるSMMCは、TRM（TamperResistant Module：耐タンパモジュール）内に暗号処理エンジン、セキュリティ鍵情報、CPU、RAM、ROM、EEPROMを備え、また、TRM外に大容量のフラッシュメモリ（例えば8MBから256MB程度）を備え、CPUが暗号処理エンジンやセキュリティ鍵情報を用いて認証処理や暗号処理等を制御し、また、外部よりダウンロードすべきプログラムを取得してTRM内に実装するEEPROMに記録して実行する。

50 【0005】ここでTRMとは、外部から本モジュール内に記録されているデータの不正な参照や改竄などを困

難にする施策が施されたモジュールである。また、フラッシュメモリには、配信対象である音楽コンテンツや動画コンテンツ等のデジタルデータが記録される。TRM内に実装するEEPROMは、他のメモリと比較して記憶容量あたりのコストが高く高価なデバイスなので、EEPROMの容量を増やすとSMMCのコストに与える影響が大きい。またデバイスの特性上、TRM内に実装するEEPROMの容量には限界があり、現状ではEEPROMの容量が64KB程度の構成が一般的である。

【0006】

【非特許文献1】「コンテンツ配信・モバイルコマース用のセキュアマルチメディアカード」日立評論2001年10月号、三宅順、石原晴次、常広隆司。

【0007】

【発明が解決しようとする課題】しかしながら、SMMCにダウンロードされるアプリケーションプログラムは今後益々増加するものと予想されるので、現状の構成ではアプリケーションプログラムを、TRM内に実装するEEPROMに格納しきれなくなるのは明らかである。

【0008】また、TRM内に実装するEEPROMの容量を超えるために記録できないアプリケーションプログラムを、TRM外に実装するフラッシュメモリに記録する方法も考えられるが、安全面を考慮すると無秩序にこのような方法を実施することはできず、少なくとも各プログラムの管理者の承認が必要であり、安全性を確保するための新たな技術の確立が望まれる。

【0009】本発明は、TRM内に実装する記憶領域の容量を超えるプログラムを、各プログラムの管理者が必要とする安全性を確保しつつ、ダウンロードすることができるセキュアデバイスを提供することを目的とする。

【0010】

【課題を解決するための手段】上記目的を達成するために、本発明に係るセキュアデバイスは、デジタルデータを格納して利用に供するセキュアデバイスであって、それぞれが記憶領域を備える複数の記憶手段と、格納先となる記憶手段を特定するための格納先情報が付加されたデジタルデータを入手する入手手段と、前記格納先情報により特定される記憶手段に前記デジタルデータを格納する処理手段とを備えることを特徴とする。

【0011】上記目的を達成するために、本発明に係る格納方法は、デジタルデータを格納して利用に供するセキュアデバイスにおける格納方法であって、前記セキュアデバイスはそれぞれが記憶領域を備え、当該格納方法は、格納先となる記憶手段を特定するための格納先情報が付加されたデジタルデータを入手する入手ステップと、前記格納先情報により特定される記憶手段に前記デジタルデータを格納する処理ステップとを含むことを特徴とする。

【0012】これらによって、デジタルデータの管理者

がデジタルデータ毎に格納先を設定しておき、TRM内に実装するEEPROMのような保護レベルが高い記憶手段の容量が足りない場合に、各デジタルデータの管理者によって設定された格納先情報に基づいて、管理者によって許可されているデジタルデータであればTRM外に実装するフラッシュメモリのような保護レベルが低い記憶手段に記録することができるので、デジタルデータを価値に応じて効率よく記録することができる。

【0013】従って、TRM内に実装する記憶領域の容量を超えるプログラムを、プログラムの管理者が必要とする安全性を確保しつつ、ダウンロードすることができる。

【0014】

【発明の実施の形態】<概要>本発明は、保護レベルの異なる複数種類の記憶領域を有するセキュアデバイスが、記憶領域を指定する付加情報を含むデジタルデータを入手して、付加情報に基づいて記憶領域の種類を特定してデジタルデータを記憶するものである。

【0015】より具体的には、保護レベルが高いEEPROMと保護レベルが低いフラッシュメモリとの2種類の記憶素子を有するSMMCにおいて、対応するプログラムを記憶すべき記憶素子がEEPROMであるかフラッシュメモリであるかを指定する付加情報を含むプログラムを、携帯電話を介してサーバから受信して、付加情報によりEEPROM及びフラッシュメモリの何れかを特定し、特定した記憶素子に対応するプログラムをダウンロードするものである。

【0016】<システム構成>図1は、本発明の実施の形態1に係るセキュアシステムの構成を示す図である。図1に示すようにセキュアシステムは、サーバ1、携帯電話2、及び、セキュアデバイス10から構成される。

【0017】サーバ1は、予めプログラム毎に付加情報を記録しておき、サーバ1の操作者による指示操作、又は、携帯電話2の利用者による要求操作に応じて、付加情報を含むプログラムを電話回線を介して携帯電話2に送信する。ここで付加情報は、例えばTRM12内に実装するEEPROM19であるかTRM12外に実装するフラッシュメモリ18であるかを指定するフラグや、記憶素子毎に設定されている保護レベルを示す数値である。

【0018】携帯電話2は、電話回線を介してサーバ1から、付加情報を含むプログラムを受信する。セキュアデバイス10は、例えばJ A V A（登録商標）Card等のダウンロード機能を備えるSMMCであり、利用者等によって携帯電話2に装着され、携帯電話2から受信された付加情報を含むプログラムを受取り、付加情報を用いてEEPROM19及びフラッシュメモリ18の何れかを特定して、特定した記憶素子にプログラムをダウンロードする。

【0019】セキュアデバイスの外形は、例えば従来の

SMMCと同様に切手大程度のサイズや、従来のICカードのサイズであり、他の形状であってもよい。図1に示すようにセキュアデバイス10は、TRM12外にカードインタフェース回路11、及び、フラッシュメモリ18を備え、TRM12内に、暗号処理エンジン13、セキュリティ鍵情報14、CPU15、ROM16、RAM17、EEPROM19、付加情報処理部20を備える。

【0020】ここでダウンロードするプログラムは、例えば、有料のアプリケーションプログラム、課金に関わるプログラム、及び、カード内に記録されているプログラムのバージョンアップ版等であり、セキュアデバイス10において相応の安全性を確保しつつ利用しなければならない。また、TRM12内に実装するEEPROM19は、格納しているプログラムに対して外部から不正なアクセスが出来ず改竄が困難であるので、本明細書において保護レベルが高いと表現する。

【0021】一方、TRM12外に実装するフラッシュメモリ18は、格納しているプログラムに対して外部から不正なアクセスが比較的容易にできるので、本明細書において保護レベルが低いと表現する。カードインタフェース回路11は、携帯電話2とデータのやり取りを行うものであり、携帯電話2から付加情報を含むプログラムを受け取る。

【0022】TRM12は、耐タンパモジュール(Tamper Resistant Module)であり、内部に記録されているデータに対する外部からの不正なアクセスや改竄を困難にする対策が施された部分である。暗号処理エンジン13は、プログラムをフラッシュメモリに格納する際に暗号化したり、プログラムの安全性を確認する為に施されたMAC情報(Message Authentication Code)やデジタル署名の認証等を行う。

【0023】セキュリティ鍵情報14は、暗号処理エンジン13による暗号処理や認証処理等に用いられる。付加情報処理部20は、カードインタフェース回路11が受け取ったプログラムに含まれる付加情報の意味を解析して、対応するプログラムの格納すべき記憶素子がEEPROM19及びフラッシュメモリ18の何れであるかを特定する。

【0024】CPU15は、予めROM16に格納されたプログラムを実行し、RAM17、フラッシュメモリ18、及び、EEPROM19を用いて、暗号処理エンジン13、及び、付加情報処理部20の制御を行い、付加情報処理部20により特定された記憶素子に、カードインタフェース回路11が受け取ったプログラムをダウンロードする。

【0025】なお、暗号処理エンジン13、及び、付加情報処理部20は、ROM16に格納されたプログラムをCPU15が実行することにより実現されるものであ

ってもよい。

(実施の形態1)

<セキュアデバイスの構成>図2は、本発明の実施の形態1に係るセキュアデバイス100の構成を示す図である。

【0026】図2に示すセキュアデバイス100は、TRM110外にプログラム入手部101、及び、低保護レベル記憶部102を備え、TRM110内に、高保護レベル記憶部118、付加情報解析部111、領域検索部112、保護レベル判定部113、移動部114、プログラム格納部115、エラー出力部116、暗号処理部117を備える。

【0027】プログラム入手部101は、図1に示したカードインタフェース回路11に相当し、携帯電話から付加情報を含むプログラムを入手する。低保護レベル記憶部102は、例えばTRM外に実装するフラッシュメモリ等の、保護レベルが低い記憶素子である。高保護レベル記憶部118は、例えばTRM内に実装するEEPROM等の、保護レベルが高い記憶素子である。

【0028】付加情報解析部111は、プログラム入手部101により入手されたプログラムに含まれる付加情報を解析して、領域検索部112、及び、暗号処理部117に動作指示を出す。領域検索部112は、プログラム入手部101により入手されたプログラムを格納できるだけの空いている記憶領域を、付加情報解析部111の指示に従って、高保護レベル記憶部118、及び、低保護レベル記憶部102から検索して、当該記憶領域が存在するか否かを判断する。

【0029】保護レベル判定部113は、領域検索部112により検索された記憶領域が、付加情報の意味に適合するかを判定することによって、プログラム入手部101により入手されたプログラムの格納場所を決定し、必要に応じてエラー情報を出力するようにエラー出力部116に指示する。図3は、本実施の形態1における付加情報を示す図である。

【0030】図3に示すように本実施の形態1においては、付加情報は5ビットとする。付加情報の下位2ビットは、“00”“01”“10”“11”の4段階の保護レベルのうちの何れかを示す。下位2ビット“00”は、対応するプログラムを高保護レベル記憶部118中の空いている記憶領域に格納すべき旨、及び、対応するプログラムを格納できるだけの空いている記憶領域が高保護レベル記憶部118中に存在しない場合には格納せずにエラー情報を携帯電話に返すべき旨を意味する。

【0031】下位2ビット“01”は、対応するプログラムを高保護レベル記憶部118中の空いている記憶領域に格納すべき旨、及び、対応するプログラムを格納できるだけの空いている記憶領域が高保護レベル記憶部118中に存在しない場合には、高保護レベル記憶部118中の記憶領域を空けて格納する旨を意味する。なお、

下位2ビット“01”は、他のプログラムが格納されている高保護レベル記憶部118中の記憶領域に上書きすべき旨を意味することにしてもよい。

【0032】下位2ビット“10”は、対応するプログラムを低保護レベル記憶部102に格納すべき旨、及び、対応するプログラムを格納できるだけの空いている記憶領域が低保護レベル記憶部102中に存在しない場合には格納せずにエラー情報を携帯電話に返すべき旨を意味する。下位2ビット“11”は、対応するプログラムを格納できるだけの空いている記憶領域が高保護レベル記憶部118中に存在する場合には高保護レベル記憶部118に格納すべき旨、存在しない場合には低保護レベル記憶部102に格納すべき旨、及び、対応するプログラムを格納できるだけの空いている記憶領域が低保護レベル記憶部102中に存在しない場合には格納せずにエラー情報を携帯電話に返すべき旨を意味する。

【0033】付加情報の下位から3ビット目は、対応するプログラムを低保護レベル記憶部102に格納する際に、暗号化するか否かを示す。ここでは下位から3ビット目“0”は、暗号化しない旨を意味し、下位から3ビット目“1”は、暗号化する旨を意味することとする。付加情報の下位から4ビット目は、対応するプログラムを低保護レベル記憶部102に格納する際に、MAC情報の付加やデジタル署名等を施すか否かを示す。

【0034】ここでは下位から4ビット目“0”は、MAC情報を付加せずデジタル署名を施さない旨を意味し、下位から4ビット目“1”は、MAC情報を付加しデジタル署名を施す旨を意味することとする。付加情報の最上位ビット（下位から5ビット目）は、セキュアデバイス100の利用者が、対応するプログラムの格納場所を自由に決めてよいか否かを示す。

【0035】ここでは最上位ビット“0”は、格納場所を自由に決めてはならない旨を意味し、最上位ビット“1”は、下位2ビットが示す保護レベルに依存することなく格納場所を自由に決めてよい旨を意味することとする。ここで保護レベル判定部113は、高保護レベル記憶部118から記憶領域が検索された場合であって、最上位ビットが“0”かつ下位2ビットが“00”、“01”、“11”の時には、検索された高保護レベル記憶部118中の記憶領域を格納場所に決定する。

【0036】また保護レベル判定部113は、低保護レベル記憶部102から記憶領域が検索された場合であって、最上位ビットが“0”かつ下位2ビットが“10”の時、及び、高保護レベル記憶部118から記憶領域が検索されずかつ低保護レベル記憶部102から記憶領域が検索された場合であって、最上位ビットが“0”かつ下位2ビットが“11”の時には、検索された低保護レベル記憶部102中の記憶領域を格納場所に決定する。

【0037】また保護レベル判定部113は、高保護レベル記憶部118と低保護レベル記憶部102との少な

くとも一方から記憶領域が検索された場合であって、最上位ビット“1”の時には、検索された何れかの記憶部中の記憶領域を格納場所に決定する。また保護レベル判定部113は、高保護レベル記憶部118から記憶領域が検索されない場合であって、最上位ビットが“0”かつ下位2ビットが“01”の時には、移動部114に高保護レベル記憶部118中の記憶領域を空ける処理を実施するよう指示する。なお、下位2ビット“01”が、他のプログラムが格納されている高保護レベル記憶部118中の記憶領域に上書きすべき旨を意味することにした場合には、他のプログラムが格納されている高保護レベル記憶部118中の記憶領域を格納場所に決定する。

【0038】また保護レベル判定部113は、高保護レベル記憶部118から記憶領域が検索されない場合であって、最上位ビットが“0”かつ下位2ビットが“00”の時、低保護レベル記憶部102から記憶領域が検索されない場合であって、最上位ビットが“0”かつ下位2ビットが“10”の時、高保護レベル記憶部118と低保護レベル記憶部102との両方から記憶領域が検索されない場合であって、最上位ビットが“1”の時、又は、最上位ビットが“0”かつ下位2ビットが“11”の時には、エラー情報を出力するようにエラー出力部116に指示する。

【0039】移動部114は、高保護レベル記憶部118から記憶領域が検索されず、付加情報の最上位ビット“0”、下位2ビットが“01”の場合に、高保護レベル記憶部118に格納されているプログラムのそれぞれに付加されている付加情報を読み出し、これら付加情報のうち、最上位ビット“0”、又は、下位2ビットが“11”である付加情報を抽出し、抽出した付加情報に対応するプログラムを低保護レベル記憶部102に移動し、プログラム入手部101により入手されたプログラムを格納するための記憶領域を高保護レベル記憶部118中に確保する。

【0040】ここで、必要な容量の記憶領域を確保できない場合には、エラー情報を出力するようにエラー出力部116に指示する。なお、必要な容量の記憶領域を確保できない場合に、他のプログラムが格納されている高保護レベル記憶部118中の記憶領域を格納場所に決定することにしてもよい。プログラム格納部115は、保護レベル判定部113により決定又は移動部114により確保された格納場所に、プログラム入手部101により入手されたプログラムを格納する。

【0041】エラー出力部116は、保護レベル判定部113によりエラー情報を出力すると決定された場合に、その旨の指示を受けてエラー情報を携帯電話に返し、携帯電話の表示部にデジタルデータを格納できない旨を提示させる。暗号処理部117は、セキュアデバイス毎に異なるID情報を保持し、プログラム入手部101により入手されたプログラムを低保護レベル記憶部1

10

20

30

40

50

02に格納する際、及び、プログラムを高保護レベル記憶部118から低保護レベル記憶部102に移動する際に、付加情報の下位から4ビット目が“1”の場合には、MAC情報を付加しデジタル署名を施し、付加情報の下位から3ビット目が“1”の場合には、保持しているID情報を用いてプログラムを暗号化する。

【0042】ここで、暗号処理部117は、プログラムを高保護レベル記憶部118に格納する際にも、付加情報の下位から4ビット目が“1”の場合には、MAC情報を付加しデジタル署名を施し、付加情報の下位から3ビット目が“1”の場合には、保持しているID情報を用いてプログラムを暗号化してもよい。

<動作>図4は、本発明の実施の形態1に係るセキュアデバイス100における、プログラムのダウンロード処理の動作を示す図である。

【0043】以下に、プログラムのダウンロード処理の動作について説明する。

(1) プログラム入手部101が、携帯電話から付加情報を含むプログラムを受け取る(S1)。

(2) 付加情報解析部111が、付加情報の最上位ビットが“0”であるか“1”であるかを解析する(S2)。

【0044】(3) 最上位ビットが“1”である場合は、領域検索部112が、プログラム入手部101により入手されたプログラムを格納できるだけの空いている記憶領域を、高保護レベル記憶部118、及び、低保護レベル記憶部102から検索して、当該記憶領域が少なくとも一方の記憶部に存在するか否かを判断する(S3)。存在しない場合は、エラー処理を行う。

【0045】(4) 存在する場合は、利用者の直接指示や利用者により予め設定されている指示等に基づいて、検索された何れかの記憶部中の記憶領域を格納場所に決定する(S4)。

(5) 最上位ビットが“0”である場合は、保護レベル判定部113が、付加情報の下位2ビットが“10”であるか否かを判定する(S5)。

【0046】(6) 下位2ビットが“10”である場合は、領域検索部112が、プログラム入手部101により入手されたプログラムを格納できるだけの空いている記憶領域が、低保護レベル記憶部102に存在するか否かを検索して、当該記憶領域が存在するか否かを判断する(S6)。存在しない場合は、エラー処理を行う。

(7) 存在する場合には、保護レベル判定部113が、検索された低保護レベル記憶部102中の記憶領域を格納場所に決定する(S7)。

【0047】(8) 下位2ビットが“10”でない場合は、領域検索部112が、プログラム入手部101により入手されたプログラムを格納できるだけの空いている記憶領域が、高保護レベル記憶部118に存在するか否かを検索して、当該記憶領域が存在するか否かを判断す

る(S8)。

(9) 存在する場合には、保護レベル判定部113が、検索された高保護レベル記憶部118中の記憶領域を格納場所に決定する(S9)。

【0048】(10) 存在しない場合には、保護レベル判定部113が、付加情報の下位2ビットが“00”であるか否かを判定する(S10)。下位2ビットが“00”である場合は、エラー処理を行う。

(11) 下位2ビットが“00”でない場合は、保護レベル判定部113が、付加情報の下位2ビットが“01”であるか否かを判定する(S11)。

【0049】(12) 下位2ビットが“01”である場合は、移動部114が、高保護レベル記憶部118に格納されているプログラムを、それぞれに付加されている付加情報に基づいて低保護レベル記憶部102に移動し、記憶領域を高保護レベル記憶部118中に確保する(S12)。確保出来ない場合にはエラー処理を行う。ここで、高保護レベル記憶部118に格納されている移動対象のプログラムに、暗号処理部117による各処理が施されていない場合には、当該プログラムの移動に際して、付加情報の下位から4ビット目に応じてMAC情報を付加しデジタル署名を施し、3ビット目に応じてプログラムを暗号化する。

【0050】(13) 下位2ビットが“01”でない場合は“11”であるので、領域検索部112が、プログラム入手部101により入手されたプログラムを格納できるだけの空いている記憶領域が、低保護レベル記憶部102に存在するか否かを検索して、当該記憶領域が存在するか否かを判断する(S13)。存在しない場合は、エラー処理を行う。

【0051】(14) 存在する場合には、保護レベル判定部113が、検索された低保護レベル記憶部102中の記憶領域を格納場所に決定する(S14)。

(15) プログラム格納部115が、決定又は確保された格納場所にプログラムを格納する(S19)。ここで、当該プログラムを低保護レベル記憶部102に格納する際には、付加情報解析部111が付加情報の下位から4ビット目及び3ビット目を解析し、暗号処理部117が、解析結果に応じてMAC情報を付加しデジタル署名を施し、またプログラムを暗号化する。

【0052】(16) 格納場所を検索又は確保できない場合には、エラー出力部116が、エラー情報を携帯電話に返す(S20)。

(実施の形態2)

<セキュアデバイスの構成>図5は、本発明の実施の形態2に係るセキュアデバイス200の構成を示す図である。

【0053】なお、実施の形態1と同様の構成要素には同一番号を付し、その説明を省略する。図5に示すセキュアデバイス200は、TRM210外にプログラム入

手部101、及び、低保護レベル記憶部102を備え、TRM210内に、高保護レベル記憶部118、付加情報解析部111、領域検索部112、保護レベル判定部213、移動部214、プログラム格納部115、エラー出力部116、暗号処理部117を備える。

【0054】保護レベル判定部213は、保護レベル判定部213は、優先度が高いプログラムから順に高保護レベル記憶部118に格納し、高保護レベル記憶部118に空き領域が足らなくなったら、低保護レベル記憶部102に格納し、必要に応じてエラー情報を出力するようにエラー出力部116に指示する。図6は、本実施の形態2における付加情報を示す図である。

【0055】図6に示すように本実施の形態2においては、付加情報は5ビットとする。付加情報の下位2ビットは、“00”“01”“10”“11”の4段階のプログラムの優先度のうちの何れかを示す。下位2ビット“00”はプログラムの優先度が最も高い事を意味する。下位2ビット“01”はプログラムの優先度が2番目に高い事を意味する。

【0056】下位2ビット“10”はプログラムの優先度が3番目に高い事を意味する。下位2ビット“11”はプログラムの優先度が4番目に高い事を意味する。付加情報の下位から3ビット目、4ビット目及び最上位ビットは、実施の形態1と同様である。ここで保護レベル判定部213は、高保護レベル記憶部118から記憶領域が検索された場合には、検索された高保護レベル記憶部118中の記憶領域を格納場所に決定する。

【0057】また保護レベル判定部213は、高保護レベル記憶部118から記憶領域が検索されなかった場合であって、付加情報の最上位ビット“0”かつ下位2ビットが“00”“01”“10”の時には、移動部214に高保護レベル記憶部118中の記憶領域を空ける処理を実施するように指示する。また保護レベル判定部213は、高保護レベル記憶部118から記憶領域が検索されず、低保護レベル記憶部102から記憶領域が検索された場合であって、付加情報の最上位ビット“0”かつ下位2ビットが“11”の時には、検索された低保護レベル記憶部102中の記憶領域を格納場所に決定する。

【0058】移動部214は、高保護レベル記憶部118から記憶領域が検索されず、付加情報の最上位ビット“0”、下位2ビットが“00”“01”“10”の場合に、高保護レベル記憶部118に格納されているプログラムのそれぞれに付加されている付加情報を読み出し、これら付加情報のうち、元の付加情報よりも優先度が低い付加情報を抽出し、抽出した付加情報に対応するプログラムを低保護レベル記憶部102に移動し、プログラム入手部101により入手されたプログラムを格納するための記憶領域を高保護レベル記憶部118中に確保する。

【0059】ここで、記憶領域を高保護レベル記憶部1

18中に確保できなかった場合には、記憶領域を低保護レベル記憶部102中に確保する。また、記憶領域を低保護レベル記憶部102中にも確保できなかった場合には、保護レベル判定部213がエラー情報を出力するようにエラー出力部116に指示する。

【0060】また、例えば、付加情報の下位から2ビット目が“0”の場合には、高保護レベル記憶部118にのみ格納を許可するように予め取り決めていたとすると、移動部214は下位から2ビット目が“0”の付加情報に対応するプログラムの移動は行わず、また、保護レベル判定部213は高保護レベル記憶部118中に記憶領域が検索されなかった場合であって、付加情報の下位から2ビット目が“0”の時には、低保護レベル記憶部102に記憶領域が検索されたとしても低保護レベル記憶部102中の記憶領域を格納場所に決定はせずに、エラー情報を出力するようにエラー出力部116に指示する。

【0061】＜動作＞図7は、本発明の実施の形態2に係るセキュアデバイス200における、プログラムのダウンロード処理の動作を示す図である。以下に、プログラムのダウンロード処理の動作について説明する。なお、実施の形態1と同様のステップには同一番号を付しその説明を省略する。

【0062】(1)実施の形態1の(1)と同じ。

(2)実施の形態1の(2)と同じ。

(3)実施の形態1の(3)と同じ。

(4)実施の形態1の(4)と同じ。

(5)最上位ビットが“0”である場合は、領域検索部112が、プログラム入手部101により入手されたプログラムを格納できるだけの空いている記憶領域が、高保護レベル記憶部118に存在するか否かを検索して、当該記憶領域が存在するか否かを判断する(S21)。

【0063】(6)存在する場合には、保護レベル判定部113が、検索された高保護レベル記憶部118中の記憶領域を格納場所に決定する(S22)。

(7)存在しない場合には、保護レベル判定部113が、付加情報の下位2ビットが“11”であるか否かを判定する(S23)。

(8)下位2ビットが“11”である場合は、領域検索部112が、プログラム入手部101により入手されたプログラムを格納できるだけの空いている記憶領域が、低保護レベル記憶部102に存在するか否かを検索して、当該記憶領域が存在するか否かを判断する(S24)。存在しない場合は、エラー処理を行う。

【0064】(9)存在する場合には、保護レベル判定部113が、検索された低保護レベル記憶部102中の記憶領域を格納場所に決定する(S25)。

(10)下位2ビットが“11”でない場合は、移動部214が、高保護レベル記憶部118に格納されているプログラムのそれぞれに付加されている付加情報を読み

10

20

30

40

50

出し、これら付加情報のうち、元の付加情報よりも優先度が低い付加情報を抽出し、抽出した付加情報に対応するプログラムを低保護レベル記憶部102に移動し、プログラム入手部101により入手されたプログラムを格納するための記憶領域を高保護レベル記憶部118中に確保する(S26)。

【0065】ここで、高保護レベル記憶部118に格納されている移動対象のプログラムに、暗号処理部117による各処理が施されていない場合には、当該プログラムの移動に際して、付加情報の下位から4ビット目に

応じてMAC情報を付加しデジタル署名を施し、3ビット目に応じてプログラムを暗号化する。

(11) 記憶領域を高保護レベル記憶部118中に確保できない場合には、記憶領域を低保護レベル記憶部102中に確保する(S27)。記憶領域を低保護レベル記憶部102中にも確保できない場合には、エラー処理を行う。

【0066】(12) 実施の形態1の(15)と同じ(S15)。

(13) 実施の形態1の(16)と同じ(S16)。

(変形例) なお、付加情報は対応するプログラムと切り離しができないように、プログラムファイルのヘッダに付加情報をプログラムIDと共に記録し、ヘッダを含むプログラムファイル全体に対して、MAC情報を付加したりデジタル署名を施し、本発明のセキュアデバイスがプログラムのダウンロードの条件として、MAC情報やデジタル署名の認証を行なってもよいし、また、プログラムを実行することにより付加情報を出力するものであってもよい。

【0067】また、本発明の実施の形態1及び2では、付加情報をプログラムと共に格納し、格納したプログラムを移動する際に用いているが、移動等を行わず格納後に付加情報を使わない場合には付加情報を格納しなくてもよいので、付加情報を除いてプログラムのみを格納しても構わない。また、本発明の実施の形態1及び2では、プログラムを格納する記憶素子として、保護レベルが異なる2種類の記憶素子を用いて説明したが、保護レベルが異なる3種類以上の記憶素子を用いても同様に実施できる。

【0068】また、本発明の実施の形態1及び2では、プログラム毎に付加情報を対応付けているが、1つのプログラムに複数の付加情報を対応付けてもよい。例えば、1つのプログラムを複数のサブプログラムに分割してサブプログラム毎に付加情報を対応付けることによって、決算プログラムの中で料金を直接処理しているような秘匿性の高いサブプログラムだけを保護レベルの高い記憶素子に格納することができる。また例えば、プログラム中のメインルーチンと各サブルーチンを分離して各ルーチン毎に付加情報を対応付け、メインルーチンを保護レベルの高い記憶素子に格納することによってプロ

ラムを難読化することができ、あるいは、各サブルーチンのうち秘匿性の高いサブルーチンだけを保護レベルの高い記憶素子に格納することができる。

【0069】また、本発明の実施の形態1及び2では、ダウンロードの対象をプログラムとして説明したが、デジタルコンテンツであってもよいし、他のデジタルデータであってもよい。

(まとめ) 以上のように、本発明のセキュアデバイスによれば、プログラムに含まれる付加情報に基づいてプログラムの格納場所を決定する事ができるので、プログラムの管理者が付加情報を予め設定しておくことによって、TRM内に実装する記憶領域の容量を越えるプログラムを、各プログラムの管理者が必要とする安全性を確保しつつ、ダウンロードすることができる。

【0070】ここで、産業上の利用の可能性という観点で考えると、本発明は、インターネット等のネットワークを介して、音楽コンテンツや動画像コンテンツの配信を受けるコンテンツ配信サービス、及び、モバイルECサービス等の様々な電子情報サービスに適用することができる。本発明のセキュアデバイスにより、TRM内に実装する記憶領域の容量を越えるプログラムを、各プログラムの管理者が必要とする安全性を確保しつつダウンロードすることができ、利用者は本発明のセキュアデバイスを自分の携帯電話に装着して、外出先からコンテンツ配信サービスやモバイルECサービス等を安全に行うことができる。

【0071】

【発明の効果】本発明に係るセキュアデバイスは、デジタルデータを格納して利用に供するセキュアデバイスであって、それぞれが記憶領域を備える複数の記憶手段と、格納先となる記憶手段を特定するための格納先情報が付加されたデジタルデータを入手する入手手段と、前記格納先情報により特定される記憶手段に前記デジタルデータを格納する処理手段とを備えることを特徴とする。

【0072】本発明に係る格納方法は、デジタルデータを格納して利用に供するセキュアデバイスにおける格納方法であって、前記セキュアデバイスはそれぞれが記憶領域を備え、当該格納方法は、格納先となる記憶手段を特定するための格納先情報が付加されたデジタルデータを入手する入手ステップと、前記格納先情報により特定される記憶手段に前記デジタルデータを格納する処理ステップとを含むことを特徴とする。

【0073】これらによって、デジタルデータの管理者がデジタルデータ毎に格納先を設定しておき、TRM内に実装するEEPROMのような保護レベルが高い記憶手段の容量が足りない場合に、各デジタルデータの管理者によって設定された格納先情報に基づいて、管理者によって許可されているデジタルデータであればTRM外に実装するフラッシュメモリのような保護レベルが低い

記憶手段に記録することができるので、デジタルデータを価値に応じて効率よく記録することができる。

【0074】従って、TRM内に実装する記憶領域の容量を越えるプログラムを、プログラムの管理者が必要とする安全性を確保しつつ、ダウンロードすることができる。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報は保護レベルを示し、前記処理手段は、前記格納先情報が示す保護レベルと同じ保護レベルが設定されている記憶手段を前記デジタルデータの格納先として特定することを特徴とすることもできる。

【0075】これによって、デジタルデータの管理者がデジタルデータ毎に保護レベルを設定しておき、保護レベルが一致する記憶手段を格納先として特定することができるので、デジタルデータを価値に応じて効率よく記録することができる。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報は保護レベルを示し、前記処理手段は、前記格納先情報が示す保護レベル以上の保護レベルが設定されている記憶手段のうちの1つを前記デジタルデータの格納先として特定することを特徴とすることもできる。

【0076】これによって、デジタルデータの管理者がデジタルデータ毎に保護レベルを設定しておき、保護レベルが同等以上の記憶手段を格納先として特定することができるので、デジタルデータを価値に応じて効率よく記録することができる。また、セキュアデバイスにおいて、前記処理手段は、前記入手手段により入手された格納先情報が示す保護レベル以上の保護レベルが設定された記憶手段のうち前記デジタルデータを格納するための空いている記憶領域を確保できる記憶手段を全て検索する検索手段と、検索手段により検索された記憶手段のうち一番高い保護レベルが設定されている記憶手段を前記デジタルデータの格納場所として決定する決定手段と、前記デジタルデータを決定手段により決定された記憶手段に格納する格納手段とを含むことを特徴とすることもできる。

【0077】これによって、空いている記憶領域を確保できる記憶手段のうち、一番高い保護レベルが設定されている記憶手段を格納先として特定することができるので、それぞれのデジタルデータをできるだけ安全に記録することができる。また、セキュアデバイスにおいて、前記処理手段は、さらに、前記検索手段により何れの記憶手段も検索されなかった場合に利用者にデジタルデータを格納できない旨を提示するためのエラー情報を出力する出力手段を含むことを特徴とすることもできる。

【0078】これによって、空いている記憶領域が無い場合に、利用者にデジタルデータを格納できない旨を提示することができる。また、セキュアデバイスにおいて、前記処理手段は、さらに、前記検索手段により何れ

の記憶手段も検索されなかった場合に、(1)前記入手手段により入手された格納先情報が示す第1保護レベル以上の保護レベルが設定されている記憶手段に格納されているデジタルデータのそれぞれに付加された格納先情報を読み出し、(2)読み出した格納先情報のうち、それぞれの格納先情報が示す保護レベルが、当該第1保護レベルよりも低い格納先情報を抽出し、(3)抽出した格納先情報に対応するデジタルデータを、当該第1保護レベルよりも低く、且つ、それぞれの格納先情報が示す保護レベル以上の保護レベルが設定されている記憶手段に移動することにより、前記入手手段により入手されたデジタルデータを格納するための記憶領域を確保する移動手段を含み、前記格納手段は、移動手段により確保された記憶領域に前記入手手段により入手されたデジタルデータを格納することを特徴とすることもできる。

【0079】これによって、先に格納されているデジタルデータを格納先情報に基づいて移動して、新しいデジタルデータを格納するための記憶領域を確保することができるので、それぞれのデジタルデータを価値に応じて効率よく記録することができる。また、セキュアデバイスにおいて、記処理手段は、さらに、前記移動手段により記憶領域を確保できない場合に利用者にデジタルデータを格納できない旨を提示するためのエラー情報を出力する出力手段を含むことを特徴とすることもできる。

【0080】これによって、先に格納されているデジタルデータを移動しても記憶領域を確保できない場合に、利用者にデジタルデータを格納できない旨を提示することができる。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報は保護レベルを示し、さらに、前記対応するデジタルデータの格納先として当該保護レベルが設定されている記憶手段のみを格納先として特定するか、及び、当該保護レベルが設定されている記憶手段以上の保護レベルが設定された記憶手段を格納先として特定するかのどちらかを指定し、前記処理手段は、前記格納先情報に従い前記格納先情報が示す保護レベルが設定されている記憶手段を、又は、前記格納先情報が示す保護レベル以上の保護レベルが設定されている記憶手段のうちの1つを前記デジタルデータの格納先として特定することを特徴とすることもできる。

【0081】これによって、保護レベルが一致する記憶手段を格納先として特定するか、保護レベルが同等以上の記憶手段を格納先として特定するかを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟性が高い。また、セキュアデバイスにおいて、前記格納先情報は前記対応するデジタルデータの格納先を当該セキュアデバイスにおいて格納する際に任意に決定してもよい可否かを指定し、前記処理手段は、前記格納先情報に従い任意に決定する記憶手段に、又は、前記格納先情報により特定される記憶手段に前記

デジタルデータを格納することを特徴とすることもできる。

【0082】これによって、格納先を当該セキュアデバイスにおいて格納する際に任意に決定してもよいかを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟性が高い。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報はデジタルデータを所定の保護レベル以下の記憶手段に格納する際に暗号化するか否かを指定し、前記処理手段は、デジタルデータを前記所定の保護レベル以下の記憶手段に格納する際に前記格納先情報に従い当該デジタルデータを暗号化して格納するか、又は、そのまま格納することを特徴とすることもできる。

【0083】これによって、デジタルデータを所定の保護レベル以下の記憶手段に格納する際に暗号化するか否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟性が高い。また、セキュアデバイス毎に固有の鍵を用いて暗号化して格納する場合には、フラッシュメモリのような保護レベルが低い記憶手段に格納したデジタルデータが、他のセキュアデバイスに不正にコピーされるといった攻撃を回避できる。

【0084】つまり、他のセキュアデバイスに不正にコピーされたとしても、鍵が異なるので正しく復号することができないため、正常に利用できない。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報はデジタルデータを所定の保護レベル以下の記憶手段に格納する際にデジタルデータに改竄検出用の情報を付加するか否かを指定し、前記処理手段は、デジタルデータを前記所定の保護レベル以下の記憶手段に格納する際に前記格納先情報に従い当該デジタルデータに改竄検出用の情報を付加して格納するか、又は、そのまま格納することを特徴とすることもできる。

【0085】これによって、デジタルデータを所定の保護レベル以下の記憶手段に格納する際に改竄検出用の情報を付加するか否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟性が高い。また、改竄検出用の情報を付加して格納する場合には、フラッシュメモリのような保護レベルが低い記憶手段に格納したデジタルデータや格納先情報が改竄されてデジタルデータが不正に用いられるといった攻撃を回避できる。

【0086】つまり、デジタルデータや格納先情報が改竄されたとしても、認証処理を行うことにより改竄されていることが解るので、改竄されている場合にはデジタルデータの使用を禁止すればよい。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報はデジタルデー

タを所定の保護レベル以下の記憶手段に格納する際にデジタルデータにデジタル署名を埋め込むか否かを指定し、前記処理手段は、デジタルデータを前記所定の保護レベル以下の記憶手段に格納する際に前記格納先情報に従い当該デジタルデータにデジタル署名を埋め込んで格納するか、又は、そのまま格納することを特徴とすることもできる。

【0087】これによって、デジタルデータを所定の保護レベル以下の記憶手段に格納する際に、デジタル署名を施すか否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟性が高い。また、デジタル署名を施して格納する場合には、フラッシュメモリのような保護レベルが低い記憶手段に格納したデジタルデータや格納先情報が改竄されてデジタルデータが不正に用いられるといった攻撃を回避できる。

【0088】つまり、デジタルデータや格納先情報が改竄されたとしても、認証処理を行うことにより改竄されていることが解るので、改竄されている場合にはデジタルデータの使用を禁止すればよい。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記格納先情報は前記デジタルデータの優先度を示し、少なくとも1つの記憶手段にはデジタルデータが格納され、記憶手段に格納されているデジタルデータにはデジタルデータの優先度が設定され、記憶手段にはより優先度が高いデジタルデータがより保護レベルが高い記憶手段に格納されている状態でデジタルデータが格納されており、前記処理手段は、前記格納先情報により示される優先度に基づいて前記状態を維持したまま前記入手手段により入手されたデジタルデータを格納することを特徴とすることもできる。

【0089】これによって、デジタルデータの管理者がデジタルデータ毎に優先度を設定しておき、優先度の高さに応じて格納先を特定することができるので、デジタルデータを効率よく記録することができる。また、セキュアデバイスにおいて、記憶手段に格納されているデジタルデータにはデジタルデータの優先度を示す格納先情報が付加されており、前記処理手段は、一番高い保護レベルが設定されている記憶手段から順に、(1)前記入手手段により入手されたデジタルデータを格納するための空いている記憶領域を確保できるか否かを判定し、

(2)判定が否定的な場合に、判定対象の記憶手段に格納されているデジタルデータのそれぞれに付加された格納先情報を読み出し、(3)読み出した格納先情報のうち、それぞれの格納先情報が示す優先度が、前記入手手段により入手された格納先情報が示す優先度よりも低い格納先情報を抽出し、(4)抽出した格納先情報を含むデジタルデータを、移動するデジタルデータ対応する保護レベルより低い保護レベルが設定されている記憶手段に移動し、(5)前記判定が肯定的となるまで(1)～

10

20

30

40

50

(4)の処理を繰り返すことにより、前記入手手段により入手されたデジタルデータを格納するための記憶領域を確保する移動手段と、移動手段により確保された記憶領域に前記入手手段により入手されたデジタルデータを格納する格納手段とを含むことを特徴とすることもできる。

【0090】これによって、先に格納されているデジタルデータを優先度に基づいて移動して、新しいデジタルデータを格納するための、できるだけ高い保護レベルが設定されている記憶領域を確保することができるので、それぞれのデジタルデータをできるだけ安全に記録することができる。また、セキュアデバイスにおいて、前記移動手段により読み出された格納先情報はデジタルデータを移動する場合に暗号化するか否かを指定し、前記移動手段は、移動すべきデジタルデータに付加された格納先情報に従い当該デジタルデータを暗号化して移動するか、又は、そのまま移動することを特徴とすることもできる。

【0091】これによって、デジタルデータを移動する際に暗号化するか否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟が高い。また、セキュアデバイス毎に固有の鍵を用いて暗号化して移動する場合には、フラッシュメモリのような保護レベルが低い記憶手段に移動したデジタルデータが、他のセキュアデバイスに不正にコピーされるといった攻撃を回避できる。

【0092】つまり、他のセキュアデバイスに不正にコピーされたとしても、鍵が異なるので正しく復号することができないため、正常に利用できない。また、セキュアデバイスにおいて、前記移動手段により読み出された格納先情報はデジタルデータを移動する場合にデジタルデータに改竄検出用の情報を付加するか否かを指定し、前記移動手段は、移動すべきデジタルデータに付加された格納先情報に従い当該デジタルデータに改竄検出用の情報を付加して移動するか、又は、そのまま移動することを特徴とすることもできる。

【0093】これによって、デジタルデータを移動する際に改竄検出用の情報を付加する否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟が高い。また、改竄検出用の情報を付加して移動する場合には、フラッシュメモリのような保護レベルが低い記憶手段に移動したデジタルデータや格納先情報が改竄されてデジタルデータが不正に用いられるといった攻撃を回避できる。

【0094】つまり、デジタルデータや格納先情報が改竄されたとしても、認証処理を行うことにより改竄されていることが解るので、改竄されている場合にはデジタルデータの使用を禁止すればよい。また、セキュアデバイスにおいて、前記移動手段により読み出された格納先情報はデジタルデータを移動する際にデジタルデータに

デジタル署名を埋め込むか否かを指定し、前記移動手段は、移動すべきデジタルデータに付加された格納先情報に従い当該デジタルデータにデジタル署名を埋め込んで移動するか、又は、そのまま移動することを特徴とすることもできる。

【0095】これによって、デジタルデータを移動する際にデジタル署名を施すか否かを、デジタルデータの管理者がデジタルデータ毎に設定することができるので、設定の柔軟が高い。また、デジタル署名を施して移動する場合には、フラッシュメモリのような保護レベルが低い記憶手段に移動したデジタルデータや格納先情報が改竄されてデジタルデータが不正に用いられるといった攻撃を回避できる。

【0096】つまり、デジタルデータや格納先情報が改竄されたとしても、認証処理を行うことにより改竄されていることが解るので、改竄されている場合にはデジタルデータの使用を禁止すればよい。また、セキュアデバイスにおいて、前記格納先情報は、さらに、保護レベルを示し、前記移動手段は、前記入手手段により入手された格納先情報が示す保護レベルより低い保護レベルが設定されている記憶手段においては前記処理を行わず、前記処理手段は、さらに、移動手段により記憶領域を確保できない場合に利用者にデジタルデータを格納できない旨を提示するためのエラー情報を出力する出力手段を含むことを特徴とすることもできる。

【0097】これによって、デジタルデータの管理者が、さらに、デジタルデータ毎に保護レベルを設定しておき、保護レベルが低い記憶手段に対しては移動処理を行わないので、デジタルデータの安全性を確保することができる。また、記憶領域を確保できない場合に、利用者にデジタルデータを格納できない旨を提示することができる。

【0098】また、セキュアデバイスにおいて、前記入手手段により入手されるデジタルデータはコンピュータプログラムであり、複数のサブプログラムを含み、サブプログラム毎に格納先情報が付加されており、前記処理手段は、サブプログラム毎にそれぞれに付加された格納先情報により特定される記憶手段に、対応するサブプログラムを格納することを特徴とすることもできる。

【0099】これによって、デジタルデータの管理者が、サブプログラム毎に格納先情報を設定しておき、格納先情報に基づいて、サブプログラム毎に格納先の記憶手段を特定することができるので、各サブプログラムの価値に応じて効率よく記録することができる。また、セキュアデバイスにおいて、前記複数の記憶手段にはそれぞれ保護レベルが設定されており、前記入手手段により入手されるデジタルデータはコンピュータプログラムであり1つのメインルーチンと複数のサブルーチンを含み、各ルーチン毎に格納先情報が付加され特にメインルーチンに付加された格納先情報は保護レベルが高い記憶

10

20

30

40

50

手段に格納すべき事を示し、前記処理手段は、ルーチン毎にそれぞれに付加された格納先情報により特定される記憶手段に、対応するルーチンを格納することを特徴とすることもできる。

【0100】これによって、デジタルデータの管理者が、ルーチン毎に格納先情報を設定しておき、格納先情報に基づいて、ルーチン毎に格納先の記憶手段を特定することができるので、各ルーチンの価値に応じて効率よく記録することができる。特に、メインルーチンを保護レベルの高い記憶素子に格納することによってプログラ

ムを難化することができる。
【0101】また、セキュアデバイスにおいて、前記入手手段により入手されるデジタルデータには、当該デジタルデータに付加された格納先情報の正当性を示し、又は、当該デジタルデータと格納先情報の対応が正しいことを示すデジタル署名が埋め込まれているか、又は、認証子が付加されており、前記処理手段は、前記デジタル署名、又は、認証子に応じた認証を実施し、当該認証が成功した場合に限り前記デジタルデータを格納すること

を特徴とすることもできる。
【0102】これによって、格納先情報とデジタルデータとが切り離せないで、安全性が高い。

【図面の簡単な説明】

【図1】本発明の実施の形態1に係るセキュアシステムの構成を示す図である。

【図2】本発明の実施の形態1に係るセキュアデバイス100の構成を示す図である。

【図3】本実施の形態1における付加情報を示す図である。

【図4】本発明の実施の形態1に係るセキュアデバイス100における、プログラムのダウンロード処理の動作を示す図である。

【図5】本発明の実施の形態2に係るセキュアデバイス200の構成を示す図である。

*

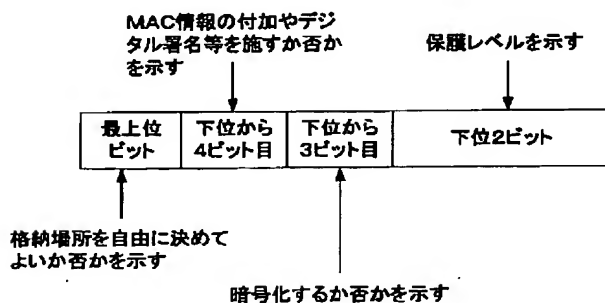
*【図6】本実施の形態2における付加情報を示す図である。

【図7】本発明の実施の形態2に係るセキュアデバイス200における、プログラムのダウンロード処理の動作を示す図である。

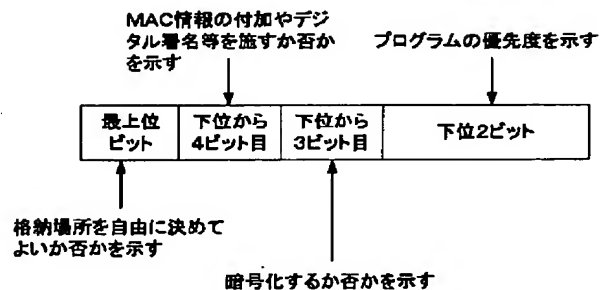
【符号の説明】

10	セキュアデバイス
11	カードインタフェース回路
12	TRM
13	暗号処理エンジン
14	セキュリティ鍵情報
15	CPU
16	ROM
17	RAM
18	フラッシュメモリ
19	EEPROM
20	付加情報処理部
100	セキュアデバイス
101	プログラム入手部
102	低保護レベル記憶部
110	TRM
111	付加情報解析部
112	領域検索部
113	保護レベル判定部
114	移動部
115	プログラム格納部
116	エラー出力部
117	暗号処理部
118	高保護レベル記憶部
200	セキュアデバイス
210	TRM
213	保護レベル判定部
214	移動部

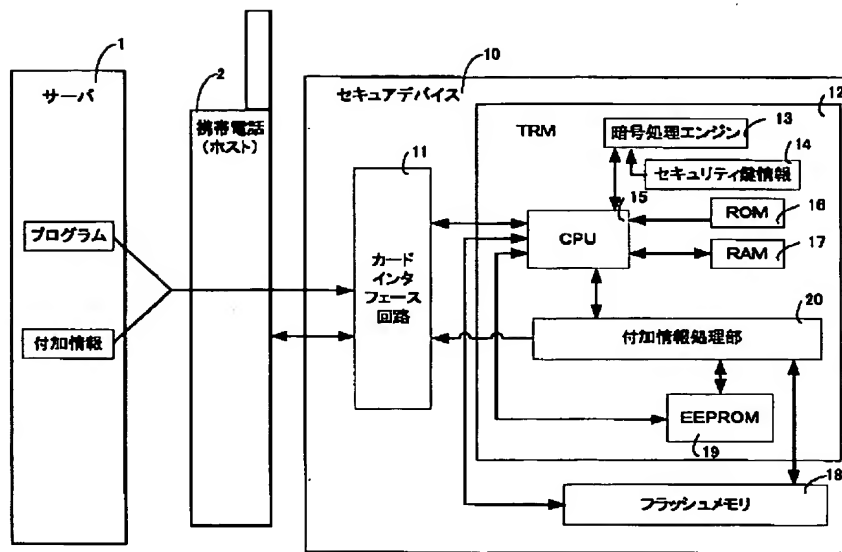
【図3】



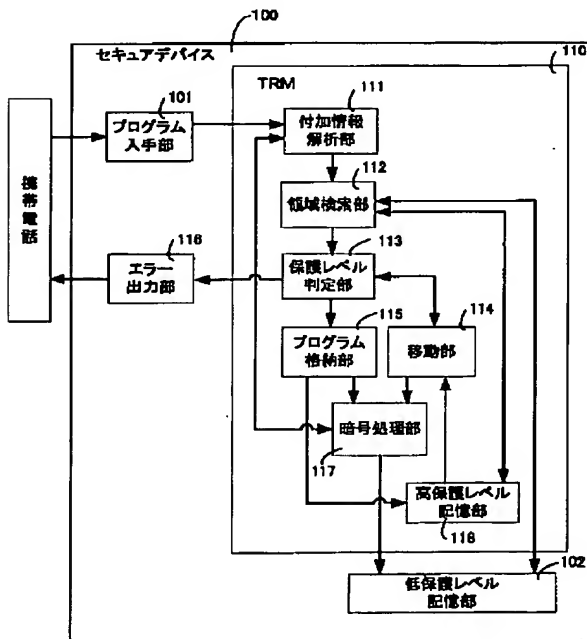
【図6】



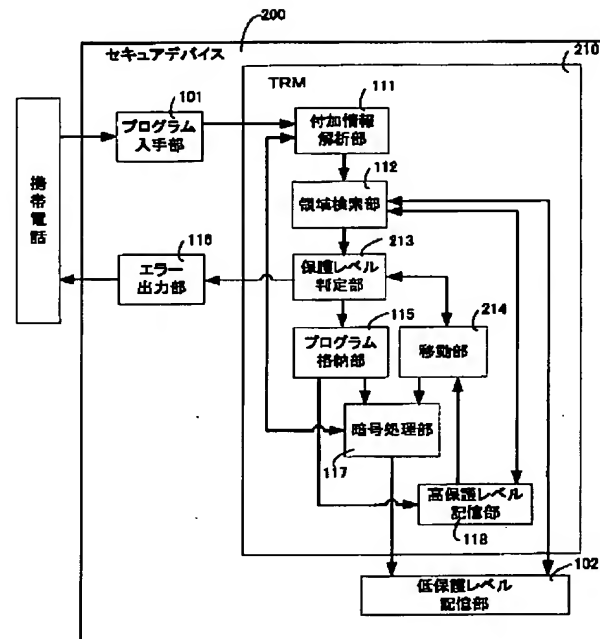
【図1】



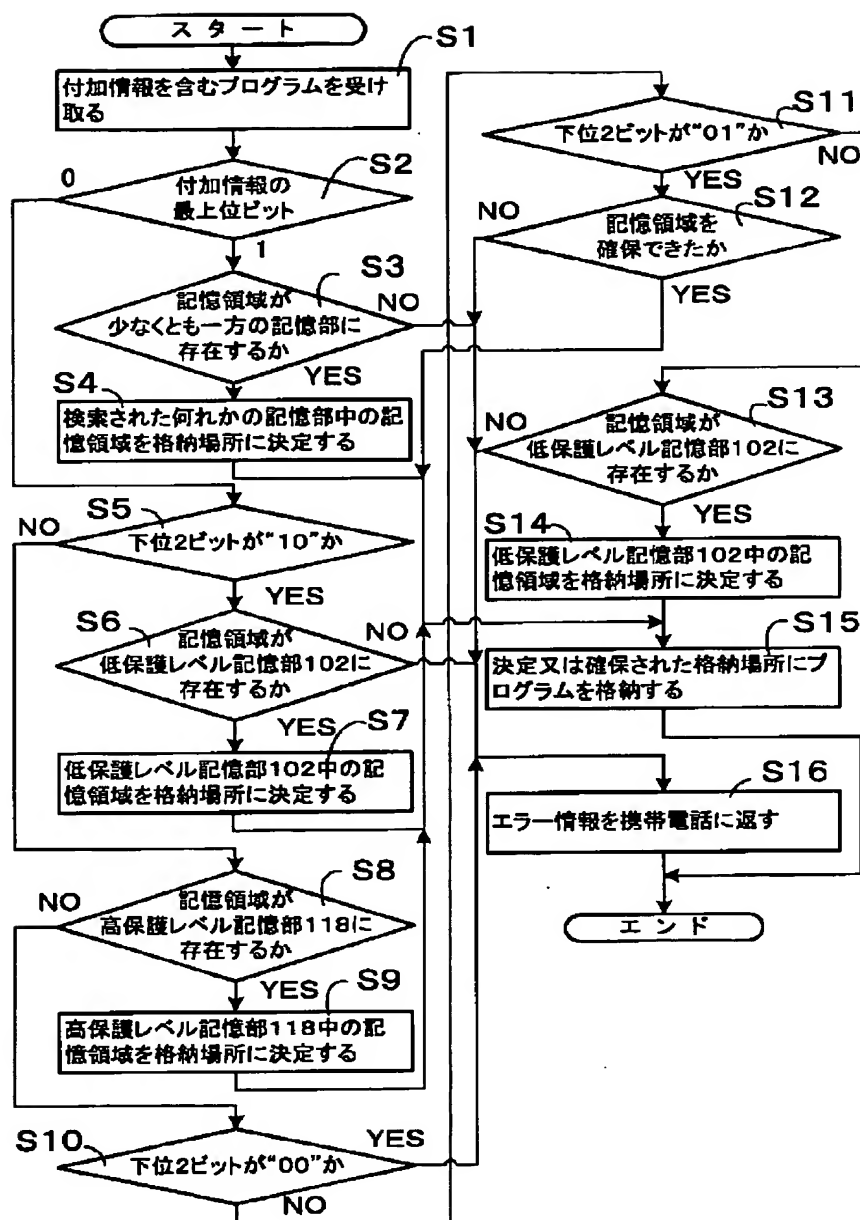
【図2】



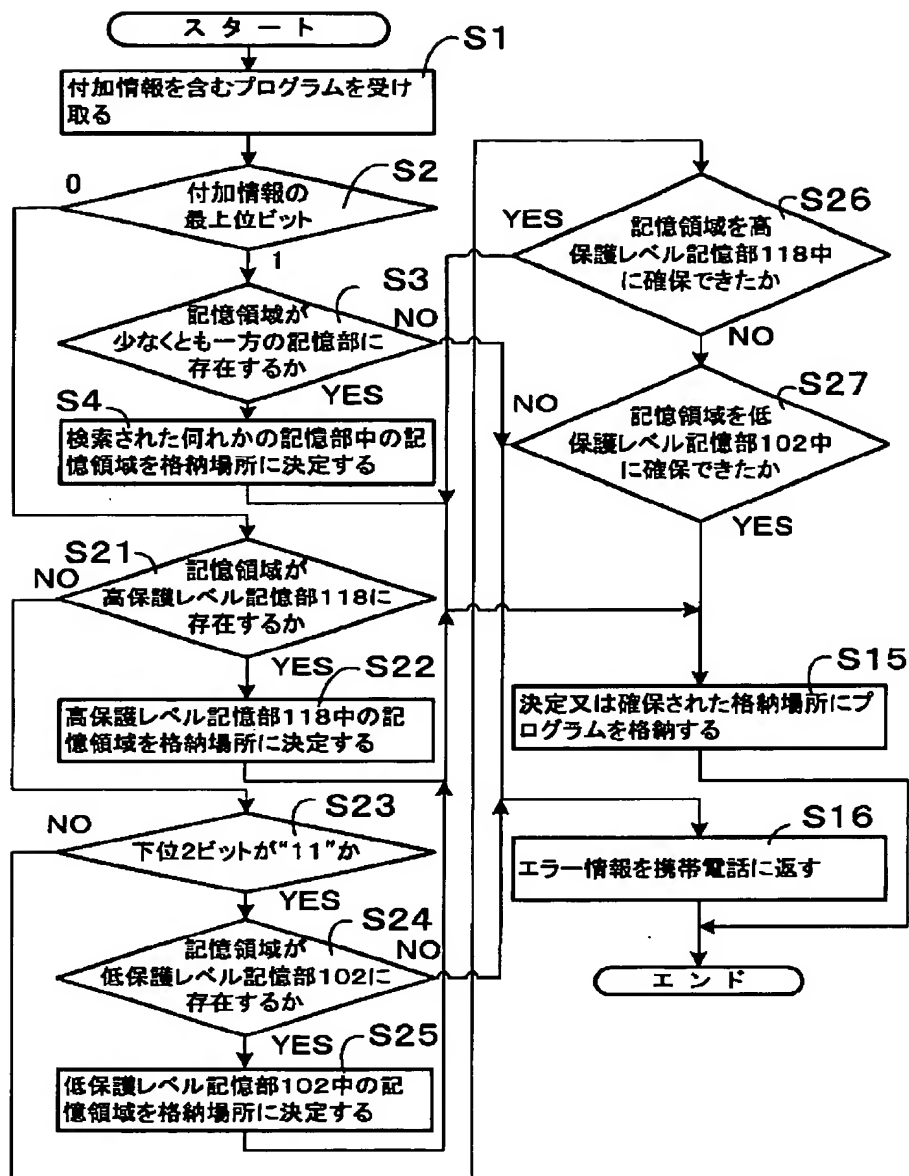
【図5】



【図4】



【図7】



フロントページの続き

(72)発明者 館林 誠
 大阪府門真市大字門真1006番地 松下電器
 産業株式会社内

Fターム(参考) 5B017 AA07 CA14 CA15
 5B035 AA00 BB09 CA11 CA29 CA38
 5B076 BB06 FB06
 5J104 AA08 AA09 AA14 AA16 DA02
 PA14